PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-080663**
(43)Date of publication of application : **11.03.2004**

(51)Int.Cl. **H04L 9/08**

(21)Application number : **2002-241447**
(22)Date of filing : **22.08.2002**

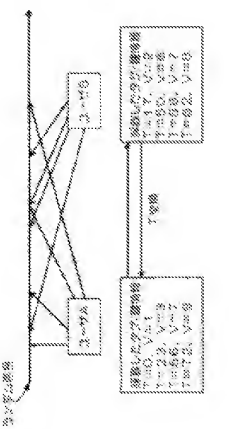
(71)Applicant : **ABEL SYSTEMS INC**
(72)Inventor : **SUZUKI FUMIO**
ITAYA SATOKO
SUZUKI AKO
MIZUKAWA SHIGEMITSU

(54) METHOD, APPARATUS, AND PROGRAM FOR GENERATING ENCODING/DECODING KEY, AND COMPUTER READABLE RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for safely acquiring an encoding key and a decoding key.

SOLUTION: The method for generating encoding/decoding key using a computer includes a step where first and second receiving parts sample random signal from a prescribed source by a prescribed method, a step where the random signal sampled by the first and second receiving parts is divided into tag information and key information, a step where the tag information acquired by the first and second receiving parts is exchanged with each other, a step where a common tag is extracted from the set of tag information exchanged between the first and second receiving parts, and a step where the first and second receiving parts generate keys for encoding and decoding using key information corresponding to the common tag.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-80663
(P2004-80663A)
(43)公開日　平成16年3月11日(2004.3.11)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601C	5J104
	H04L	9/00	601A	

審査請求 未請求　請求項の数 16　OL　（全 23 頁）

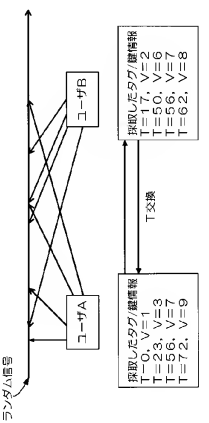
(21)出願番号　特願2002-241447(P2002-241447)
(22)出願日　平成14年8月22日(2002.8.22)

(71)出願人　500404258
アーベル・システムズ株式会社
京都府京都市西京区大枝北沓掛町二丁目３番地の１６
(74)代理人　100104949
弁理士　豊栖　康司
(74)代理人　100074354
弁理士　豊栖　康弘
(72)発明者　鈴木　文雄
京都府京都市西京区大枝北沓掛町二丁目３番地の１６
(72)発明者　板谷　聡子
大阪府箕面市如意谷４　６　１７　２０１

最終頁に続く

(54)【発明の名称】暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体

(57)【要約】
【課題】安全に暗号化鍵および復号鍵を取得する方法を提供する。
【解決手段】電子計算機を使った暗号化／復号鍵の鍵生成方法は、第１および第２の受信部がそれぞれ所定のソースからランダム信号を所定の方法でサンプリングするステップと、第１および第２の受信部がそれぞれサンプリングしたランダム信号をタグ情報と鍵情報に分割するステップと、第１および第２の受信部がそれぞれ取得したタグ情報を相互に交換するステップと、第１および第２の受信部がそれぞれ交換されたタグ情報の集合から共通するタグを抽出するステップと、第１および第２の受信部がそれぞれ共通するタグと対応する鍵情報を使って暗号化および復号のための鍵を生成するステップとを有する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電子計算機を用いる暗号化もしくは復号のための鍵の生成方法であって、
第１および第２の受信部がそれぞれ所定のソースからランダム信号を所定の方法でサンプリングするステップと、
前記第１および第２の受信部がそれぞれサンプリングしたランダム信号をタグ情報と鍵情報に分割するステップと、
前記第１および第２の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、
前記第１および第２の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、
前記第１および第２の受信部がそれぞれ前記共通するタグと対応する鍵情報を使い所定の方法で鍵を生成するステップと、
を備える暗号化／復号鍵の鍵生成方法。
【請求項２】
暗号化もしくは復号のための鍵生成方法において、
第１および第２の受信部がそれぞれ所定のソースからランダム信号をブロックとして所定の方法でサンプリングするステップと、
前記第１および第２の受信部がそれぞれサンプリングした前記ブロックの一部をタグ情報として抽出するステップと、
前記第１および第２の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、
前記第１および第２の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、
前記第１および第２の受信部がそれぞれ前記共通するタグと対応するブロックの一部または全体を鍵情報として、前記鍵情報を用いて所定の方法で鍵を生成するステップと、
を有することを特徴とする暗号化／復号鍵の鍵生成方法。
【請求項３】
前記鍵生成方法はさらに、
前記第１および第２の受信部がタグ情報から生成されたタグで、共通に持つタグと対応する鍵情報を複数組み合わせて鍵を合成するステップを有することを特徴とする請求項１または２記載の暗号化／復号鍵の鍵生成方法。
【請求項４】
前記鍵生成方法はさらに、
前記第１および第２の受信部が共通のタグ情報から生成されたタグと対応する鍵情報に対して、共通部分の鍵情報の抽出を行いその結果を相互に交換するステップを有することを特徴とする請求項１から３のいずれかに記載の暗号化／復号鍵の鍵生成方法。
【請求項５】
前記鍵生成方法はさらに、
前記第１および第２の受信部がそれぞれ共通のタグ情報から生成されたタグ以外のタグ、およびこれと対応する鍵情報を鍵生成に使用しないものと判定するステップを有することを特徴とする請求項１から４のいずれかに記載の暗号化／復号鍵の鍵生成方法。
【請求項６】
前記鍵生成方法はさらに、
前記第１および第２の受信部がランダム信号のサンプリングを開始するに先立ち、第１の受信部が第２の受信部に鍵の取得開始を通知するステップを有することを特徴とする請求項１から５のいずれかに記載の暗号化／復号鍵の鍵生成方法。
【請求項７】
前記第１および第２の受信部がランダム信号のサンプリングを予め設定された方法で行うことを特徴とする請求項１から６のいずれかに記載の暗号化／復号鍵の鍵生成方法。

【請求項８】
前記第１の受信部、または第２受信部がサーバであることを特徴とする請求項１から７のいずれかに記載の暗号化／復号鍵の鍵生成方法。
【請求項９】
前記第１および第２の受信部がソースからランダム信号をサンプリングするための伝送媒体と、相互にタグ情報から生成されたタグを交換するための伝送媒体が別個の伝送媒体であることを特徴とする請求項１から８のいずれかに記載の暗号化／復号鍵の鍵生成方法。
【請求項１０】
前記ランダム信号を発生させる回数が制限されていることを特徴とする請求項１から９のいずれかに記載の暗号化／復号鍵の鍵生成方法。
【請求項１１】
暗号化もしくは復号のための鍵生成装置において、
ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングし、サンプリング情報からタグ情報と鍵情報を取得するためのサンプリング手段と、
取得したタグ情報から生成されたタグを他の生成装置と相互に交換するためのタグ交換手段と、
前記タグ交換手段で交換されたタグ集合から他の生成装置との間で共通するタグを抽出するためのタグ選択手段と、
前記共通するタグと対応する鍵情報を使って所定の方法で鍵を生成する鍵生成手段と、
を備えることを特徴とする暗号化／復号鍵の鍵生成装置。
【請求項１２】
前記サンプリング手段が、
受信されたランダム信号からこれを採取するランダム信号採取部と、
受信されたランダム信号をタグ情報と鍵情報に分割する分割部と、
分割されたタグ情報と鍵情報を格納するためのタグ／鍵情報格納メモリと、
ランダム信号を採取する動作を制御する制御部と、
を備えることを特徴とする請求項１１記載の暗号化／復号鍵の鍵生成装置。
【請求項１３】
前記サンプリング手段が、
ランダム信号を受信するランダム信号受信部と、
前記ランダム信号受信部で受信されたランダム信号を所定の期間連続的に格納するランダム信号格納メモリと、
前記ランダム信号格納メモリに格納されたランダム信号を採取するランダム信号採取部と、
採取されたランダム信号をタグ情報と鍵情報に分割する分割部と、
分割されたタグ情報と鍵情報を格納するためのタグ／鍵情報格納メモリと、
ランダム信号を採取する動作を制御する制御部と、
を備えることを特徴とする請求項１１または１２記載の暗号化／復号鍵の鍵生成装置。
【請求項１４】
前記分割部が、
受信したランダム信号を信号の種類に応じて分割するためのスプリッタと、
前記スプリッタで分割された信号にフィルタリングするためのフィルタと、
前記フィルタを通したアナログ信号をデジタル信号に変換するＡ／Ｄ変換手段と、
を備えることを特徴とする請求項１１から１３のいずれか記載の暗号化／復号鍵の鍵生成装置。
【請求項１５】
暗号化もしくは復号のための鍵生成プログラムにおいて、コンピュータに
ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングする機能と、
サンプリングしたランダム信号からタグ情報と鍵情報を取得する機能と、

取得したタグ情報から生成されたタグを他の鍵生成プログラムと相互に交換するステップと、
交換されたタグ集合から他の鍵生成プログラムとの間で共通するタグを抽出するステップと、
前記共通するタグと対応する鍵情報を使って鍵を生成するステップと、
を実現させるための暗号化／復号鍵の鍵生成プログラム。
【請求項１６】
請求項１５記載の暗号化／復号鍵の鍵生成プログラムを記録したコンピュータで読取可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明が属する技術分野】
本発明は、暗号化もしくは復号のために使用する鍵を安全に生成できる暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体に関する。例えば、鍵の生成装置やプログラムを使った暗号化システムの使用方法、利用方法を提案する。
【０００２】
【従来の技術】
近年のネットワーク技術の飛躍的な発達とインターネット接続の爆発的な普及により、電子データによる情報のやりとりが一般化している。電子データをネットワークを介してやりとりする機会が増大すると共に、送受信される電子データの漏洩、解読を防止するセキュリティ技術の重要性が高まっている。特に電子メールの送付や電子ファイルの交換、あるいは電子商取引における個人情報の暗号化などの局面においては、個人情報や金銭に関する情報など秘密情報の漏洩を防止するためのセキュリティが重要となる。
【０００３】
一般に応用が容易なセキュリティ技術としては、データの暗号化が利用されている。暗号化の方式としては、暗号化と復号（暗号解読）に同一の鍵を用いる対称鍵暗号が利用されている。しかしながらこの方式ではひとたび鍵を盗まれると第三者が容易に解読でき、秘密情報が完全に筒抜けになってしまうという欠点があった。
【０００４】
このため、暗号化と復号に別々の鍵を用いる安全性の高い暗号方式として、公開鍵暗号方式が開発、利用されている。公開鍵暗号方式では、送信者と受信者が個別の公開鍵と秘密鍵の対をそれぞれ持っている。公開鍵は公開されており、送信に先立って例えば両者の間で電子メールなどにより交換したり、公開ウェブサーバからダウンロードするなどして入手する。そして送信者は受信者の公開鍵で暗号化した情報を送信する。暗号化された情報を受信した受信者は、受信者が秘密に持っている秘密鍵を使ってこれを復号する。公開鍵暗号を採用する方法として、例えばＰＧＰ（Ｐｒｅｅｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）があり、１０２４ビットなどの高い堅牢性を誇り、フリーで利用できるバージョンが公開されていることなどから広く利用されている。さらにその他の方式としてはＰＫＣＳ（Ｐｕｂｌｉｃ　Ｋｅｙ　ＣｒｙＰｔｏｇｒａＰｈｙ　Ｓｔａｎｄａｒｄｓ）やＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）、Ｓ／ＭＩＭＥ（Ｓｅｃｕｒｅ／ＭｕｌｔｉＰｕｒＰｏｓｅ　Ｉｎｔｅｒｎｅｔ　Ｍａｉｌ　Ｅｘｔｅｎｓｉｏｎｓ）などが利用されている。
【０００５】
【発明が解決しようとする課題】
しかしながら、公開鍵暗号を含めたいずれの暗号化方式でも安全性が完全に保証されるものではない。暗号化された情報の解読は暗号化方式が高度になるほど、いいかえると鍵長のビット数が多くなるほど困難となる。しかしこれは暗号解読により時間がかかるだけのものであって、絶対に解読できないというものではない。またユーザは、暗号化もしくは復号するための鍵を予め交換する必要があるため、鍵を傍受される（盗まれる）可能性が

あり、これを使って暗号を解読される危険が依然として存在している。例えば同一の鍵を何度も使用している場合、鍵を盗まれたりして鍵が第三者の手に渡る危険性がある。鍵と暗号化された情報が（暗号文）第三者の手に渡ると、第三者は容易に暗号文を解読できる。あるいは安全性の低い鍵を使用すると、いくつかの暗号文から鍵そのものを知られてしまうことにもなる。いうなれば、安全性の低い鍵で情報を暗号化したとしても、その暗号文は暗号知識を有する者にとって暗号化されていない（平文）秘密情報と同等である。

【０００６】

本発明は、従来の暗号化技術が持つ根本的な問題、すなわち暗号化もしくは復号のための鍵の交換プロセスに注目し、この段階での鍵の漏洩を防止することを目的に開発されたものである。本発明の主な目的は、暗号化／復号鍵の鍵配信の際に第三者に傍受される事態を回避するシステムを提供し、鍵の漏洩を防止し暗号解読に対して安全性の高い暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を提供することにある。

【０００７】

【課題を解決するための手段】

上記課題を解決するための本発明の請求項１に記載される発明は、暗号化もしくは復号のための暗号化／復号鍵の鍵生成方法に関するものである。この鍵生成方法は、第１および第２の受信部がそれぞれ所定のソースからランダム信号を所定の方法でサンプリングするステップと、前記第１および第２の受信部がそれぞれサンプリングしたランダム信号をタグ情報と鍵情報に分割するステップと、前記第１および第２の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、前記第１および第２の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、前記第１および第２の受信部がそれぞれ前記共通するタグに対応する鍵情報を使って所定の方法で鍵を生成するステップとを有することを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【０００８】

また、本発明の請求項２に記載される暗号化／復号鍵の鍵生成方法は、第１および第２の受信部がそれぞれ所定のソースからランダム信号をブロックとして所定の方法でサンプリングするステップと、前記第１および第２の受信部がそれぞれサンプリングした前記ブロックの一部をタグ情報として抽出するステップと、前記第１および第２の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、前記第１および第２の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、前記第１および第２の受信部がそれぞれ前記共通するタグに対応するブロックの一部または全体を鍵情報として、前記鍵情報を用いて所定の方法で暗号化／復号鍵の鍵を生成するステップとを有することを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【０００９】

さらに、本発明の請求項３に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１または２に記載される特徴に加えて、さらに前記第１および第２の受信部が共通するタグに対応する鍵情報を複数組み合わせて鍵を合成するステップを有することを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１０】

さらにまた、本発明の請求項４に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から３のいずれかに記載される特徴に加えて、さらに前記第１および第２の受信部がタグ情報から生成されたタグで、共通のタグに対応する鍵情報に対して、鍵情報の共通部分の抽出を行い、その結果を相互に交換するステップを有することを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１１】

さらにまた、本発明の請求項５に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から４のいずれかに記載される特徴に加えて、さらに前記第１および第２の受信部がそ

れぞれ共通するタグ情報から生成されたタグ以外のタグおよびこれと対応する鍵情報を鍵生成に使用しないものと判定するステップを有することを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１２】

さらにまた、本発明の請求項６に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から５のいずれかに記載される特徴に加えて、さらに前記第１および第２の受信部がランダム信号のサンプリングを開始するに先立ち、第１の受信部が第２の受信部に鍵の取得開始を通知するステップを有することを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１３】

さらにまた、本発明の請求項７に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から８のいずれかに記載される特徴に加えて、前記第１および第２の受信部がランダム信号のサンプリングを予め設定された方法で行うことを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１４】

さらにまた、本発明の請求項８に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から７のいずれかに記載される特徴に加えて、前記第１または第２の受信部がサーバであることを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１５】

さらにまた、本発明の請求項９に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から８のいずれかに記載される特徴に加えて、前記第１および第２の受信部がソースからランダム信号をサンプリングするための伝送媒体と、相互にタグ情報から生成されるタグを交換するための伝送媒体が別個の伝送媒体であることを特徴とする。前記第１および第２の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【００１６】

さらにまた、本発明の請求項１０に記載される暗号化／復号鍵の鍵生成方法は、上記請求項１から９のいずれかに記載される特徴に加えて、前記ランダム信号を発生させる回数が制限されていることを特徴とする。

【００１７】

一方、本発明の請求項１１に記載される発明は、暗号化もしくは復号のための鍵生成装置に関するものである。この鍵生成装置は、ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングし、サンプリング信号からタグ情報と鍵情報を取得するためのサンプリング手段と、取得したタグ情報から生成されたタグを他の生成装置と相互に交換するためのタグ交換手段と、前記タグ交換手段で交換されたタグ集合から他の生成装置との間で共通するタグを抽出するためのタグ選択手段と、前記共通するタグと対応する鍵情報を使って所定の方法で鍵を生成する鍵生成手段とを備えることを特徴とする。

【００１８】

また、本発明の請求項１２に記載される暗号化／復号鍵の鍵生成装置は、上記請求項１１に記載される特徴に加えて、前記サンプリング手段が、受信されたランダム信号からこれを採取するランダム信号採取部と、受信されたランダム信号をタグ情報と鍵情報に分割する分割部と、分割されたタグ情報と鍵情報を格納するためのタグ／鍵情報格納メモリと、ランダム信号を採取する動作を制御する制御部とを備えることを特徴とする。

【００１９】

さらにまた、本発明の請求項１３に記載される暗号化／復号鍵の鍵生成装置は、上記請求項１１または１２に記載される特徴に加えて、前記サンプリング手段が、ランダム信号を受信するランダム信号受信部と、前記ランダム信号受信部で受信されたランダム信号を所定の期間連続的に格納するランダム信号格納メモリと、前記ランダム信号格納メモリに格納されたランダム信号を採取するランダム信号採取部と、採取されたランダム信号をタグ情報と鍵情報に分割する分割部と、分割されたタグ情報と鍵情報を格納するためのタグ／

鍵情報格納メモリと、ランダム信号を採取する動作を制御する制御部とを備えることを特徴とする。

【００２０】

さらにまた、本発明の請求項１４に記載される暗号化／復号鍵の鍵生成装置は、上記請求項１１から１３のいずれかに記載される特徴に加えて、前記分割部が、受信したランダム信号を信号の種類に応じて分割するためのスプリッタと、前記スプリッタで分割された信号にフィルタリングするためのフィルタと、前記フィルタを通したアナログ信号をデジタル信号に変換するＡ／Ｄ変換手段とを備えることを特徴とする。

【００２１】

また、本発明の請求項１５に記載される発明は、暗号化もしくは復号のための鍵生成プログラムに関するものである。この暗号化／復号鍵の鍵生成プログラムは、コンピュータに、ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングする機能と、サンプリングしたランダム信号からタグ情報と鍵情報を取得する機能と、取得したタグを他の暗号鍵生成プログラムと相互に交換するステップと、交換されたタグ集合から他の鍵生成プログラムとの間で共通のタグ情報から生成されたタグを抽出するステップと、前記共通するタグと対応する鍵情報を使って鍵を生成するステップとを実現させるためのプログラムである。

【００２２】

さらにまた、本発明の請求項１６に記載されるコンピュータで読取可能な記録媒体は、上記請求項１５に記載される前記暗号化／復号鍵の鍵生成プログラムを記録したものである。記録媒体には、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷやフレキシブルディスク、磁気テープ、ＭＯ、ＭＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ、ＤＶＤ＋Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷなどの磁気ディスク、光ディスク、光磁気ディスク、半導体メモリその他のプログラムやデータなどを格納可能な媒体が含まれる。またプログラムがネットワークを介してダウンロード可能として配布する形態も包含する。

【００２３】

従来の考え方では、どのようにして暗号化／復号鍵の鍵を解読され難くするかというアプローチで安全性を高める技術が開発されていた。これに対し本発明は、各ユーザがそれぞれ異なる位置、時間においてランダム信号をサンプリングし、これを利用して暗号化／復号鍵の鍵を生成するという別の観点から開発されたものである。特に鍵やその元となるデータ自体を交換しないことによって、例え通信を傍受されたとしても鍵を入手、再現されることはない。鍵を生成するアルゴリズムは既存の方法が利用できるため、本発明を様々な暗号化システムに利用してより安全性の高いデータ交換や配信が実現される。

【００２４】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。ただし、以下に示す実施の形態は、本発明の技術的思想を具体化するための暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を例示するものであって、本発明は暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を以下のものに特定しない。

【００２５】

またこの明細書は、特許請求の範囲に示される部材を、実施の形態の部材に特定するものでは決してない。なお、各図面が示す部材の大きさや位置関係などは、説明を明確にするため誇張していることがある。さらに、本発明を構成する各要素は、複数の要素を同一の部材で構成して一の部材で複数の要素を兼用する態様としてもよい。

【００２６】

本明細書において電子計算機には、いわゆるコンピュータに限られず、システムＬＳＩやＣＰＵ、ＭＰＵやその他のＩＣを使用した装置、回路その他の組み込み機器や素子自体を包含する意味で使用する。

【００２７】
本明細書において暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システムおよび暗号化／復号鍵の鍵生成プログラムは、暗号化／復号鍵の鍵生成における鍵の生成や鍵の送信動作そのもの、ならびに生成された鍵の利用など暗号化／復号鍵の鍵生成に関連する入出力、表示、演算、通信その他の処理をハードウェア的に行う装置や方法に限定するものでない。ソフトウェア的に処理を実現する装置や方法も本発明の範囲内に包含する。例えば汎用の回路やコンピュータにソフトウェアやプログラム、プラグイン、オブジェクト、ライブラリ、アプレット、コンパイラ、モジュール、特定のプログラム上で動作するマクロなどを組み込んで鍵生成などを実施可能とした汎用あるいは専用のコンピュータ、ワークステーション、端末、携帯型電子機器、ＰＤＣ、ＣＤＭＡ、ＧＳＭ、ＩＭＴ２０００や第４世代などの携帯電話、ＰＨＳ、ＰＤＡ、ページャ、スマートフォンその他の電子デバイスも、本発明の暗号化／復号鍵の鍵生成方法および暗号化／復号鍵の鍵生成システムに含まれる。また本明細書においては、プログラム自体も暗号化／復号鍵の鍵生成システムに含むものとする。さらに本明細書においてプログラムとは、単体で使用されるものに限られず、特定のコンピュータプログラムやソフトウェア、サービスなどの一部として機能する態様や、必要時に呼び出されて機能する態様、ＯＳなどの環境において サービスとして提供される態様、環境に常駐して動作する態様、バックグラウンドで動作する態様やその他の支援プログラムという位置付けで使用することもできる。

【００２８】
本発明の実施例において使用されるコンピュータなどの端末同士、およびサーバやこれらに接続される操作、制御、入出力、表示、各種処理その他のためのコンピュータ、あるいはプリンタなどその他の周辺機器との接続は、例えばＩＥＥＥ１３９４、ＲＳ－２３２ＸやＲＳ－４２２、ＵＳＢなどのシリアル接続、パラレル接続、あるいは１０ＢＡＳＥ－Ｔ、１００ＢＡＳＥ－ＴＸ、１０００ＢＡＳＥ－Ｔなどのネットワークを介して電気的に接続して通信を行う。接続は有線を使った物理的な接続に限られず、ＩＥＥＥ８０２．１１Ｘなどの無線ＬＡＮやＢｌｕｅｔｏｏｔｈなどの電波、赤外線、光通信などを利用した無線接続などでもよい。さらにデータの交換や設定の保存などを行うための記録媒体には、メモリカードや磁気ディスク、光ディスク、光磁気ディスク、半導体メモリなどが利用できる。

【００２９】
また本明細書においては、特に断りのない限り「暗号化」とはデータの暗号化と共に、暗号化されたデータの復号または暗号解読を含むものとする。

【００３０】
上述のように、暗号化／復号鍵の鍵は傍受される危険が伴う。送信者と受信者間で鍵を交換する際、インターネットのようなオープンなネットワークを介して鍵が送信される以上、第三者の傍受の可能性は常にある。これを防止するために専用回線を介して鍵を交換したり、記録メディアに保存して物理的に交換するなどの手段もあるが、いずれも手間がかかる。これらの方法と比較すると、電子データによるネットワークを介した鍵の交換が最も簡単かつ迅速な手段であることは明らかである。よって、インターネットなどの高速に利用できるネットワーク回線を利用することを前提として、安全に鍵を生成する方法を確立することが情報通信技術において極めて重要となる。

【００３１】
現在、安全性の高い鍵配信方法として、量子（Ｑｕａｎｔｕｍ：１量子の動き）を利用した鍵配信方法が提案されている［Ｃ．Ｂｅｎｎｅｔｔ，Ｆ．Ｂｅｓｓｅｔｔｅ，Ｇ．Ｂｒａｓｓａｒｄ，Ｌ．Ｓａｌｖａｉｌ，Ｊ．Ｓｍｏｌｉｎ，“ＥＸＰｅｒｉｍｅｎｔａｌ Ｑｕａｎｔｕｍ ＣｒｙＰｔｏｇｒａＰｈｙ”，Ｊｏｕｒｎａｌ ｏｆ ＣｒｙＰｔｏｌｏｇｙ，Ｖｏｌ．５，Ｎｏ．３，１９９２］。この方法では、配信された鍵を傍受している第三者が存在することを検知することができる。

【００３２】
しかしながら、この方法を実現するには単一量子を扱うことのできる装置が必要で、単一

量子を扱うための特殊な装置は実施化が技術的に難しいという問題があった。量子を利用した技術には、例えば特開２００１－７７９８号公報などがある。

【００３３】

さらに、上記問題を解決する手段として、情報理論的に安全な方法が提案されている［C. Cachin and U. Maurer, "Unconditional Security Against Memory-Bounded Adversaries", Advances in Cryptology CRYPTO '97, B. Kaliski (Ed.), Lecture Notes in Computer Science, Vol. 1294, Springer-Verlag, 1997, PP. 292-306; Y. Aumann and M. O. Rabin, "Information Theoretically Secure Communication in the Limited Storage Space Model", Advances in Cryptology CRYPTO '99, M. J. Wiener (Ed.), Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, 1999, PP. 65-79］。この方法は、データの送信者と受信者が同一のソースから送出される乱数列をサンプリングして、これを鍵として使用する方法である。仮に、送信者と受信者がソースから送出される乱数列からデータを採取している時間内に、ソースから送信されるデータの数をN^P、送信者と受信者が採取できるデータの数をN^Sとする。ここで、サンプリング数が極めて多く、また、ソースから送出される乱数の量がサンプリング数より十分に多いと仮定すると、$N^P >> N^S >> 1$となる。このとき、受信者と送信者で、一回のサンプリング毎に一致しているデータの総数の期待値は$(N^S/N^P) \times N^S = N^{2S-P}$である。

【００３４】

この暗号化／復号鍵のサンプリングの際に、同一のソースから送出される乱数列を同様にサンプリングする第三者すなわち盗聴者が存在する場合を考える。同時に第三者が乱数列から採取できるデータ数も、送信者や受信者と同レベルと考えるのが一般的であるので、N^Sとする。このとき、送信者と受信者で一致した乱数データを第三者が共通して所有する一致しているデータの総数の期待値は$(N^{2S-P}/N^P) \times N^S = N^{3S-2P}$である。つまり、$N^S$と$N^P$の値を適切に調整することにより、第三者が送信者・受信者と共通のデータを持つ期待値を限りなく０に近づけることができる。例えば、送信者Ａと受信者Ｂのサンプルが一致する数の期待値をN_{AB}と、送信者Ａと受信者Ｂと第三者Ｅのサンプルが一致する数の期待値をN_{ABE}となるようにするため、$N^P = N_{AB}^3/N_{ABE}^2$、$N^S = N_{AB}^2/N_{ABE}$とすればよい。このシステムは、ソースから大量に純粋な乱数が発生されるのに対し、乱数を採取する側、すなわち送信者と受信者と第三者において、乱数採取を行うシステムが一部の数のサンプルしかできないことを前提としている。このシステムでは、従来のように暗号化／復号に同じ鍵を何度も用いることなく、特定の乱数を鍵として一回だけ暗号化／復号に用いるため、鍵を盗まれにくく秘匿性を高めることができる。

【００３５】

しかしながら、上記の報告例は理論の提案に止まり、具体的に実施化するためのモデルが提示されていない。具体的には、ランダム信号からデータをどのようにして取り出し、また取り出したデータが共通のものであることをどのようにして認識するかといった点が明らかにされていない。

【００３６】

そこで本発明者らは鋭意研究を重ねた結果、この提案を具体的に実現する方法を発明し、秘匿性の高い暗号化／復号鍵の鍵生成システムを開発するに至った。本システムでは、多変量ランダム信号、多変ビットランダム信号または複合ランダム信号からタグと鍵を取得する。このシステムでは、離れた者同士が鍵を交換することなくランダム信号を共有することができ、このランダム信号を鍵情報として利用する。このようにして取得した鍵は、

そのまま暗号化乱数としても利用できるし、またはより高度な暗号化の鍵やＩＤのようなものとしても用いることもできる。

【００３７】

また様々な暗号やセキュリティシステムに実装して利用する形態も考えられる。応用分野の一例としては、モバイルシステム、ポイント・トゥ・ポイント（Ｐｏｉｎｔ－ｔｏ－Ｐｏｉｎｔ：ＰｔｏＰ）システムや無線ＬＡＮ、ＵＷＢでイーサーネット（登録商標）を用いたユーザ間のやり取りなどが挙げられる。

【００３８】

以下、本発明の実施例を使って、ユーザＡとユーザＢが共通の鍵を入手する手法を説明する。共通の鍵を安全に取得したユーザＡとユーザＢは、この鍵を使って暗号化／復号を行い安全なやりとりを行うことができる。図１は本発明の１実施例に係る暗号化／復号鍵の鍵取得方法で各ユーザがランダム信号をサンプリングする様子を時系列的に示したものである。このシステムは、図２に示すように、ランダム信号を発生するソース１と、伝達媒体２とを備え、ランダム信号のソースとユーザＡとユーザＢが伝達媒体２に接続している。ユーザＡ、Ｂはそれぞれランダム信号のソース１からランダム信号列をサンプリングし、得られたランダム信号をそれぞれタグ情報Ｔと鍵情報Ｖに分割する。そしてタグ情報Ｔのみを相互に交換し、共通するタグ情報Ｔと対応する鍵情報Ｖのみを残しこれを用いて鍵を生成する。ここで図１のようなタグ情報Ｔ、鍵情報Ｖをユーザ Ａ、Ｂがそれぞれ取得したとすれば、Ｔ＝５６と対応するＶ＝７のみを残す。

【００３９】

図２の例では、ソース１は純粋なランダム信号を連続的に発生させるランダム信号源である。ソース１はランダム信号を発生させるものであれば何でもよい。ソース１はランダム信号を伝達媒体２を介して送出する。伝達媒体２は、通信が可能な媒体であればよく、ＬＡＮ、インターネット網や電話線などの公衆回線や専用回線が使用できる。接続方式や通信方式も限定されず、イーサネット（登録商標）、シリアル、パラレル、ＩＥＥＥ１３９４、ＵＳＢなどが利用でき、媒体は銅線ケーブルや光ファイバーなど、通信に適したものであればよい。また物理的な媒体を使って電気信号を伝達する手段に限られず、電波、無線ＬＡＮ、Ｂｌｕｅｔｏｏｔｈなど無線による通信や赤外線通信、光通信など、信号をやりとりできるあらゆる手段を含む。

【００４０】

また図２の例では、伝達媒体がランダム信号を送出するランダム信号線と、後述するようにユーザＡとユーザＢがタグ情報を交換、比較するためのタグ情報通信線を兼ねている。ただ、図３に示すようにランダム信号線２αとタグ情報通信線２ｂを個別に設けてもよい。この場合は複数の回線もしくはチャンネルを使用してデータのやりとりをするため、通信傍受がより困難になるというメリットがある。例えば、ランダム信号線をインターネット回線とし、タグ情報通信線を電話回線とする。もちろん、有線通信と無線通信を混在させることも可能であることはいうまでもない。

【００４１】

ユーザＡとユーザＢは、伝達媒体２を介してランダム信号のソース１から送信されるランダム信号を採取することができる。各ユーザは、ランダム信号をサンプリングするサンプリング手段３を備える。サンプリング手段３の一例を図４および図５に示す。図４に示すサンプリング手段３は、ランダム信号受信部８と、ランダム信号採取部４と、分割部５と、タグ／鍵情報格納メモリ６と、制御部７を備える。このサンプリング手段３はシステムＬＳＩなどで構成できる。また、ランダム信号受信部８は、サンプリング手段３と外部で接続されてもよい。ランダム信号受信部８は所定の方法あるいはタイミングで、ランダム信号のソース１からランダム信号を連続的に取得する。取得するランダム信号はブロックまたは波形パターンとしてランダム信号採取部４で採取され、分割部５に送出する。分割部５は、採取したランダム信号をタグ情報Ｔと鍵情報Ｖに分割し、分割された各タグ／鍵情報をタグ／鍵情報格納メモリ６に格納する。図１２にブロック状のランダム信号列をタグ情報と鍵情報に分割する様子を示す。同じタグ情報が二度と現れない確率を十分小さく

するためには、タグ情報部分がある程度の長さを備えることが好ましい。以上の動作によってユーザはタグ情報Ｔと鍵情報Ｖを得ることができる。ランダム信号を採取する動作は、制御部７により制御される。制御部７は、制御変数としてサンプリングレート、シーケンス、ゲートなどを有している。

【００４２】

ここで分割部の一例を図６に示す。この図に示す分割部は、スプリッタ９と、フィルタ１０と、Ａ／Ｄ変換手段１１を備える。分割部は受信したランダム信号をスプリッタ９で信号の種類に応じて分割し、フィルタ１０を通じてＡ／Ｄ変換手段１１に送られる。フィルタ１０は波長フィルタ、周波数フィルタ、時間遅延などが使用され、フィルタ１０を通じたアナログ信号をＡ／Ｄ変換手段１１によりデジタル信号に変換する。このようにして採取したランダム信号を二つのランダム信号に分割した後、デジタル信号に変換し、デジタル情報としてタグ情報Ｔと鍵情報Ｖに分割し、タグ／鍵情報格納メモリ６に格納する。

【００４３】

一方、図５に示すサンプリング手段３は、ランダム信号受信部８Ｂと、ランダム信号格納メモリ１２と、ランダム信号採取部１３と、タグ／鍵情報格納メモリ６Ｂと、分割部５Ｂと、制御部７Ｂを備える。また、ランダム信号受信部８Ｂは、サンプリング手段３と外部で接続されてもよい。このサンプリング手段３も、システムＬＳＩなどで構成できる。サンプリング手段３は、ランダム信号受信部８Ｂでランダム信号を受信し、ランダム信号格納メモリ１２に所定の期間連続的に格納する。ランダム信号格納メモリ１２は、レジスタなどで構成できる。ランダム信号格納メモリ１２に格納されたランダム信号から、ランダム信号採取部１３がランダム信号として採取し、分割部５Ｂに送る。分割部５Ｂは上記図４と同様、受信したランダム信号をタグＴと鍵Ｖに分割し、分割された各情報をタグ／鍵情報格納メモリ６Ｂに格納する。これによってユーザはランダム信号としてタグＴと鍵Ｖを得ることができる。ランダム信号を採取する動作は、上記と図４と同様に制御部７Ｂにより制御される。制御部７Ｂは、制御変数としてサンプリングレート、シーケンス、ゲートなどを有している。

【００４４】

以上のサンプリング手段３を使って、各ユーザは所定のタイミングで、ソース１から送出されるランダム信号のサンプリングを開始する。そしてサンプリングした情報をタグＴと鍵に分割する。ここでサンプリングとは、所定のタイミングでソース１より送られてくるランダムな信号を、所定の方法で測定することを指すものとする。ランダム信号のサンプリングにより最終的にタグＴと鍵Ｖを得る手法としては、図７、図８などの方法が利用できる。

【００４５】

図７に示すサンプリング方法は、サンプリングを行うタイミングをタイミング信号生成部１４で決定する。この方法では、タイミング信号生成部１４でタイミング信号を発生するタイミングで、ランダム信号をランダム信号受信部８Ｃによりサンプリングし、Ａ／Ｄ変換手段１１ＣでＡ／Ｄ変換した後分割部５Ｃでタグ Ｔと鍵Ｖに分割する。

【００４６】

また図８に示す方法は、上記の方法のようにサンプリングした値をＡ／Ｄ変換した後にタグ情報と鍵情報に分割するのでなく、先にランダム信号をアナログ信号のまま分割部５Ｅでタグ信号と鍵信号とに分割しておき、分割されたタグ信号および鍵信号をそれぞれランダム信号受信部８Ｅでサンプリングして Ａ／Ｄ変換手段１１ＥでＡ／Ｄ変換し、タグＴと鍵Ｖをそれぞれ得るものである。図８（ａ）に示す方法によって得られるタグ信号、鍵信号、タイミング信号の波形を図９に、また図８（ｂ）に示す方法によって得られる各波形を図１０に、それぞれ示す。これらの方法では、ランダム信号を図９（ａ）に示すチャンネル１のタグ信号と、図９（ｂ）に示すチャンネル２の鍵信号に分割している。そしてタイミング信号生成部１４Ｅで生成された図９（ｃ）に示すタイミング信号のパルスがトリガとなって、この時点での値がそれぞれサンプリングされる。

【００４７】

なお信号を分割する方法は様々な手法が利用でき、例えばランダム信号を２つに分割する、異なる波長で分割するなどが挙げられる。あるいは分割でなく、相関のない２つのランダム信号を用意して、特定の時間における信号をそれぞれタグ信号、鍵信号とすることもできる。例えば図１０に示すようにチャンネル１とチャンネル２の２つのランダム信号のソース１Ａ、１Ｂを用意し、一方をタグ信号のサンプリング用、他方を鍵信号のサンプリング用として利用する。この例では、図１０（ｃ）のような所定の信号をトリガ信号として、図１０（ｄ）のタイミング信号を発生する。図１０（ｃ）の信号が所定の　値を超える、または所定のパターンが検出されたときをトリガとして、図１０（ａ）、（ｂ）に示すように、トリガ時のランダム信号の値をそれぞれタグ信号、鍵信号としてサンプリングする。

【００４８】

さらに３つ以上のランダム信号を用いて、複数のランダム信号を組み合わせるなどの処理を加えることで新たなランダム信号を生成し、これをタグ信号や鍵信号とする、あるいはタグ信号と鍵信号に分割することもできる。

【００４９】

以上のようにして、サンプリング手段３によりサンプリングしたデータからタグＴと鍵Ｖを得ている。タグＴは送信者と受信者間で交換するもので、鍵Ｖは実際に使用する鍵となる。ただ、タグと鍵を決定する手法はこれ以外にも採用でき、例えばサンプリングした全体のランダム信号を鍵情報とし、ランダム信号の一部をタグ情報として用いてもよい。

【００５０】

［実施例１］

実施例１として、ユーザＡとユーザＢ間の１：１の通信を考える。この場合、図１１に示すフローチャートのような処理を行って暗号化／復号鍵の鍵を生成することができる。

【００５１】

まずステップＳ１でユーザＡ、ユーザＢはそれぞれランダム信号のソース１からサンプリングを開始する。サンプリングの開始は、各ユーザＡ、ユーザＢ間でサンプリングを開始する旨を何らかの手段で通知することもできるが、予め定められた所定の時間あるいは周期でそれぞれ開始してもよい。サンプリング動作は各ユーザＡ、ユーザＢが同期を取ることなく任意に行う。所定の回数または時間のサンプリングが終了すると、ステップＳ２に進む。

【００５２】

ステップＳ２では、お互いが取得したランダム信号の集合からタグ情報を交換する。タグ情報は各ユーザＡ、ユーザＢがそれぞれ取得したランダム信号から抽出し、複数の時間におけるそれぞれのタグ情報を送出する。次にステップＳ３に進む。

【００５３】

ステップＳ３では、交換したタグの内から共通するタグ情報を所定数含んでいるかどうかを確認する。共通するタグ情報が含まれていない場合、あるいは所定数の共通タグ情報に達していないときは、ステップＳ１に戻って再度サンプリングを行う。このとき、すでに取得したタグ情報および対応する鍵情報は鍵生成に使用しないものと判定し、破棄してもよいし、共通タグ情報と対応する鍵情報のみを保持していてもよい。共通するタグ情報が所定数含まれている場合は終了する。

【００５４】

ステップＳ３の処理の後、共通するタグ情報に対応する鍵情報が正当であるかどうかのチェックを行うこともできる。ユーザＡとユーザＢがそれぞれの鍵情報に基づいて所定のビット列を計算し、タグ情報と共に相互に交換する。例えばハッシュ関数を用いて［Ｔｉ，Ｈ（Ｖｉ）］を交換する。これによって、タグ情報部分が一致しているにも拘わらず、鍵情報が異なるようなランダム信号を排除したり、エラーチェックを行うことができる。

【００５５】

また、ステップＳ３の処理の後、暗号化／復号鍵の鍵生成を行うこともできる。鍵生成方法は、複数の鍵情報を組み合わせて行うこともできる。安全性を高めるために複数のタグ

情報および鍵情報を組み合わせる様子を図１３に示す。図１３では４ビットのタグ情報または鍵情報を複数列組み合わせて、４ｍビットのタグ、鍵をそれぞれ得ている。暗号化／復号鍵の鍵生成には、既知のプロトコルが使用できる。このようにして暗号化／復号鍵の鍵が生成されたことをユーザ同士で通知する。このときユーザ間で互いに送信、チェックを行ってもよいし、ユーザＡがタグ情報やビット列をユーザＢに送信し、ユーザＢ側のみでチェックを行ってもよい。

【００５６】

［実施例２］

次に、ユーザが複数存在する場合にこれらのユーザ間で暗号化／復号鍵の鍵を生成する例について説明する。複数ユーザ間の通信では、図１４のように１：ｎで各々が通信する場合と、図１５のように特定のサーバを介して通信を行う場合が考えられる。まず、図１４のようにユーザＡ、ユーザＢ、ユーザＣの三者間でやりとりする実施例２の場合について説明する。基本的な手順は上述の実施例１と同様の手順となる。この場合ステップ２においては、ユーザＡ、ユーザＢ、ユーザＣはそれぞれ自分以外の相手とタグ情報のやり取りをし、３者間で共通のタグ情報を共通タグとして保持する。複数のユーザが共通のタグを取得できる期待値は、ユーザ数ｎが大きくなるにつれ小さくなる。

【００５７】

［実施例３］

さらに、図１５に示すように複数のユーザ（ユーザ１、２、・・・、ｎ）が特定のサーバを介して通信を行う例を実施例３として説明する。この図においてはユーザ間に位置するサーバと、クライアントに相当する各ユーザとの間でそれぞれ通信を行う形態となる。ユーザは他のユーザとの通信を行う際、直接ユーザ間で通信するのでなく一旦サーバを介して行うこととなる。この形態ではサーバと各ユーザとの間は１：１の通信となるため、基本的には実施例１と同様の手順で暗号化／復号鍵の鍵を生成する。その際、実施例２と異なり共通のタグを取得できる期待値はユーザ数に拘わらず一定となる。なお、ここでサーバとは分散処理システムにおいて他のユーザからの要求に応じて暗号化に関するサービスを提供するものの意味であって、例えば特定のユーザにこの役割をさせることもできる。

【００５８】

さらにこの形態では、図１６に示すようにタグテーブルを用意して各ユーザ間の通信で通信相手に対する暗号化／復号鍵の鍵をそれぞれ特定し、安全性を保持することができる。図１６の例では、ユーザ１とユーザ２との間でタグテーブルを図のように設定している。例えば、サーバがユーザ１と通信する場合はタグＴ＝３を共通タグとして採用し、サーバとユーザ２が通信する場合はタグＴ＝８を使用する。また、ユーザ１とユーザ２が通信する場合、サーバはユーザ１とユーザ２で共通するタグとしてＴ＝２を使用する。このようにして、ローカルなユーザ間の通信はサーバへ共通タグ情報を問い合わせ、対応する鍵情報により、ユーザ間でサーバを介して通信することができる。このため、すべてのユーザが相互にタグ情報の交換を行う必要はなく、サーバと各ユーザ間のやり取りだけでデータ通信を行うことができる。さらに、サーバから特定のユーザや複数のユーザで構成されたグループに対して、暗号化された情報を送信する際に、共通な鍵情報を得ることにより一度の暗号化で送信することができる。このとき、特定のユーザやグループ以外では共通ではない鍵を用いて暗号化されたデータであるため、サーバと通信しているすべてのユーザに向けて送信されたとしても、他のユーザは正当な鍵を持っていないのでこの情報を復号することができない。これによって、各ユーザへのデータ配信の際にも、通信相手以外のユーザに対しては情報の漏洩が防止され高い秘匿性が維持される。

【００５９】

［実施例４］

さらにまた、サーバ・クライアント型のローカルな接続形態は、図１７のようなネットワーク同士の接続にも応用することができる。この場合も実施例３、４と同様のシステムを導入して秘匿性を図ることができる。

【００６０】

以上のシステムでは、タグ情報および鍵情報の元となる全てのランダム信号を、第三者が受信できないことが前提となる。有限の時間内のサンプリングといった、ランダム信号から限られた範囲のサンプリングのみが可能なシステムにおいて、送信者および受信者がタグ情報を交換することによって共通の鍵情報を見出すものである。したがって、システムのセキュリティを向上させるという面からは、ランダム信号の発生量が受信者あるいは第三者のランダム信号取得能力よりも大きい程セキュリティが高いことになる。

【００６１】

さらに傍受の危険を回避するため、ランダム信号の発行回数を制限することも可能である。ユーザが共通のランダム信号を受信すると、それ以上はランダム信号を発行しないように設定すれば、第三者がこれらのユーザと共通のランダム信号を取得することができなくなる。例えば、２者間の通信においてランダム信号を２回以上発行しないシステムとする。これによれば、情報の交換を行うユーザがそれぞれランダム信号を取得しようとしてランダム信号発生源にアクセスすると、ランダム信号発生源はランダム信号を発行するが、その発行回数を２回までに制限するのである。そうすると、ユーザが共通のランダム信号を受信すると、それ以上は同じランダム信号が発行されないので、仮に第三者が同じランダム信号にアクセスしようとしても、既に２回発行されたランダム信号を取得することはできない。このように、ランダム信号の発行回数を制限することによって、第三者によって同じランダム信号が傍受される危険を回避することができる。この方法は、例えば図１５のようにサーバを介するシステムに利用すれば特定の２者間の通信に限られず、サーバを介して複数のクライアント間での通信が可能となる。また、このようなランダム信号の発行回数の制限には、ランダム信号発生源がランダム信号を発行する毎にフラグを設定し、フラグが２つまでランダム信号を発行できるように制限する方法などが利用できる。さらにサーバがランダム信号発生源をコントロールしてもよい。

【００６２】

［暗号化方式への実装］

以上のようにしてランダム信号から共通に取得された鍵情報は、暗号化／復号のための鍵情報として用いることができ、ユーザ間で鍵そのものを交換することなく、従来の方式よりもより安全な暗号化／復号の鍵更新が実現する。また取得された鍵情報は鍵生成に使用するばかりでなく、暗号化のための乱数としても用いることができ、さらにその暗号化のための乱数を生成する種、例えば擬似乱数生成器の初期値としても用いることができる。そのほか複数個の鍵情報を合成して新たな鍵情報を生成することもできる。

【００６３】

従来、暗号化／復号鍵の鍵を更新するには鍵そのものを何らかの方法でユーザ間で交換、あるいはサーバから配信、あるいは通信を行わない物理的な手段で更新する必要がある。インターネットなどオープンなネットワークを介して配信すると、漏洩の危険に晒されるため、公開鍵暗号などを利用した鍵配信方法を用いてユーザ間で交換、あるいはサーバから配信せざるを得ない。また、通信を行わない物理的な手段、例えば、フレキシブルディスクや磁気テープなどの記録媒体にデータを記憶して交換する方法が採られている。あるいはより高度な方法として、例えばネットワークにログインするパスワードを生成するために乱数を利用する方法が利用されている。この方法では、乱数発生器を内蔵し、乱数を表示可能なスマートカードやＩＣカードを用意し、これをサーバに挿入するなどして物理的に接続する。これによってカードはサーバから乱数発生器の種を受ける。カードはユーザに物理的に配布される。乱数発生器は所定の周期で乱数を発生させるので、ユーザはログインする時点で表示されている乱数をパスワードとして利用する。この方法では定期的にパスワードとなる乱数が更新されるため、より高い安全性が確保される。

【００６４】

しかしながら、いずれの方法も記録媒体やカードを使用して物理的に配布する工程が必要となり、このことが手間となっていた。これに対し本発明を利用すれば、従来不可能であった乱数の種をリモートで更新することが可能であり、物理的に鍵自体を交換するというリスクも冒すことなく安全に鍵を更新することが可能となる。また得られた暗号化および

復号のための鍵の使用は、一回切りとする使い捨て方式（Ｏｎｅ－ｔｉｍｅ　Ｐａｄ）とすれば、より安全性を高めることもできる。もちろん、鍵を複数回使用する形態にも利用できることはいうまでもない。

【００６５】

以下、様々な暗号化方式に本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を応用した例について説明する。

【００６６】

［ストリーム（バーナム）暗号化方式］

ストリーム暗号化方式では鍵系列（乱数系列）を用意し、暗号化に際して、平文系列のｎビット目と鍵系列のｎビット目の排他的論理和を取り、これを暗号文系列とする。一方、復号に際しては、暗号化と同じ鍵系列と同様の処理を行うことにより、平文系列を取り出す。本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を用いることにより、ストリーム暗号化方式に用いる鍵系列を生成するための初期値を、第三者に知られることなく保持することができる。また、最終的に排他的論理和をとるための鍵系列として本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用することもできる。以下、ストリーム暗号化方式を利用した例として、乱数生成部分にカオスを利用したＧＣＣ暗号化方式およびＨＤＣＰ暗号化方式に本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を実装した例を説明する。

【００６７】

［ＧＣＣ暗号化方式］

ストリーム暗号化方式では、その安全性は主としてこの鍵系列として用いる乱数系列の性質に依存する。そこで、各種解読方法に対する強さが期待されているのがカオスの初期値に対する敏感な依存性を利用したカオス暗号化方式である。カオス暗号化方式は、例えば特開平０７－３３４０８１号公報、米国特許第５６９６８２６号公報などに記載される。

【００６８】

ＧＣＣ暗号化方式は、ストリーム暗号化方式の乱数生成部にカオス信号発生器を利用した暗号化方式である。このカオス信号発生器は複数のカオス発生関数からなる。入力された鍵に演算を施すことにより、使用するカオス発生関数番号、パラメータ、初期値を決定し、その値を用いてカオス信号を発生する。このカオス信号系列と平文系列の排他的論理和演算を取ることにより、これを暗号文系列とする。ここで本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、ＧＣＣ暗号化方式に用いる鍵を第三者に知られることなく更新または生成することができる。

【００６９】

［ＨＤＣＰ暗号化方式］

ＨＤＣＰ（Ｈｉｇｈ－ｂａｎｄｗｉｄｔｈ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）暗号化方式は、デジタル・ビジュアル・インターフェース（Ｄｉｇｉｔａｌ　Ｖｉｓｕａｌ　Ｉｎｔｅｒｆａｃｅ）からの出力を保護するために、インテル社が提案し、既に製品化されている技術である。このシステムでは、暗号化のためのＨＤＣＰサイファー（ＨＤＣＰ　Ｃｉｐｈｅｒ）モジュールを持つ。このモジュールでは、線形フィードバックレジスタに蓄えたデータを入れ替え規則に従って　　することにより２４ビットの擬似乱数データを生成する。この入れ替え操作に秘密デバイス鍵が用いられる。このシステムに本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、ＨＤＣＰ暗号化方式で使用される線形フィードバックレジスタに与える初期値、またはＨＤＣＰ機器が必要とする秘密デバイス鍵の更新に応用することができる。

【００７０】
このように、ストリーム暗号化方式に本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、図１８に示すように鍵系列（乱数系列）を生成するための種として、または安全な鍵生成および鍵更新を行うことができる。また、暗号化のための乱数系列として本発明で生成されるランダム信号を用いることができることはいうまでもない。さらにまた、ＡＧＣＰなどデジタル画像配信のスクランブル用、またはストリーム暗号化方式のＬＦＳＲやＯＦＢモード、ＣＦＢモードにも本発明を応用することができる。
【００７１】
［ブロック暗号化方式］
次にブロック暗号化方式への実装について、図１９に基づいて説明する。一般にブロック暗号化方式では、Ｆｅｉｓｔｅｌの開発した暗号で用いられたインボリューション（ｉｎｖｏｌｕｔｉｏｎ）と呼ばれる１：１変換ランダム処理テクニックが用いられる。その操作内容を決定するためには、暗号化／復号鍵の鍵、または鍵から導出される複数のサブ鍵が用いられる。ここで本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体により得られた鍵を、ブロック暗号化方式の暗号化／復号鍵、または複数のサブ鍵として用いることができる。
以下、ブロック暗号化方式を利用した例として、ＤＥＳ暗号とＣＡＳＴ暗号に、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を実装した例を説明する。
【００７２】
［ＤＥＳ暗号化方式］
ＤＥＳ（Ｄａｔａ　ＥｎｃｒｙＰｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号化方式は、現在世界中で最も広く使われている暗号化方式である。ＤＥＳ暗号化方式は１６段の変換部からなり、各段に用いるサブ鍵の生成は、ユーザから取得したパリティビットを含む６４ビット鍵に対して複雑な処理を加えることで行われる。本発明は、ＤＥＳ暗号化方式のための６４ビット秘密鍵や、その鍵から生成されるサブ鍵として用いることができる。本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、ＤＥＳ暗号化方式の鍵として用いることができる。
【００７３】
［ＣＡＳＴ暗号化方式］
ＣＡＳＴ暗号化方式は、エントラスト・テクノロジーズ（Ｅｎｔｒｕｓｔ　Ｔｅｃｈｎｏｌｏｇｉｅｓ）が開発した暗号化方式である。各段階の換字、転置関数および鍵スケジュール処理を工夫することで、ＤＥＳ暗号化方式よりも効果的に設計されている。本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体は、ＣＡＳＴ暗号化方式の暗号化および復号の鍵を取得するために用いることができる。以上のように、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体をブロック暗号に利用すると、ブロック暗号化方式の鍵を安全に取得できる。
【００７４】
【発明の効果】
以上説明したように、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、安全に暗号化／復号の鍵を生成することができる。それは、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体が、鍵そのものをユーザ間で交換することなく、鍵情報と対応するタグ情報を使ってやりとりを行うからである。しかもタグ情報や鍵

情報はランダムに、ランダム信号のソースから採取するため再現性がない。また各ユーザはどのランダム信号が鍵情報として使用するか、採取する時点で決定することは不可能である。鍵情報の決定は、共通するタグ情報を抽出した以降となる。第三者においては、仮に交換されるタグ情報を傍受したとしても、タグに対応する鍵情報を事前に獲得していなければ、正当な鍵を得ることができない。また鍵情報は再現性のないランダム信号から採取されるため事後的に鍵情報を再現することはできない。鍵情報を得られない限り、復号あるいは暗号解読は計算理論上、鍵情報を得た時よりもはるかに困難となる。このように、本発明を既存の暗号化システムに利用することで第三者に暗号化／復号鍵を傍受される事態を回避して、安全性の高いデータのやりとりを実現することができるのである。

【図面の簡単な説明】

【図１】本発明の一実施例に係る暗号化／復号鍵の取得方法によりランダム信号をサンプリングする様子を時系列的に示した模式図である。

【図２】本発明の一実施例に係る暗号化／復号鍵の取得方法を構成する概略図である。

【図３】本発明の他の実施例に係る暗号化／復号鍵の取得方法を構成する概略図である。

【図４】ランダム信号をサンプリングするサンプリング手段の一例を示すブロック図である。

【図５】ランダム信号をサンプリングするサンプリング手段の他の例を示すブロック図である。

【図６】分割部の一例を示すブロック図である。

【図７】ランダム信号のサンプリング構成の一例を示すブロック図である。

【図８】さらにランダム信号のサンプリング構成の他の例を示すブロック図である。

【図９】図８（ａ）に示すサンプリング構成でサンプリングを行うタイミングを示すチャートである。

【図１０】図８（ｂ）に示すサンプリング構成でサンプリングを行うタイミングを示すチャートである。

【図１１】ランダム信号をサンプリングして暗号化／復号鍵を生成する工程を示すフローチャートである。

【図１２】ブロックのランダム信号をタグ情報と鍵情報に分割する様子を示す概念図である。

【図１３】複数のタグ情報から鍵情報を組み合わせて、暗号化および復号のための鍵を構成する様子を示す概念図である。

【図１４】複数のユーザ間で暗号化／復号鍵を生成する構成を示す概念図である。

【図１５】複数のユーザ間でサーバを介して暗号化／復号鍵を生成する構成を示す概念図である。

【図１６】タグテーブルに基づいて複数のユーザ間で暗号化／復号鍵を決定する様子を示す概念図である。

【図１７】図１５の接続形態を複数のネットワーク間に拡張した様子を示す概念図である。

【図１８】本発明の実施例をストリーム暗号化方式に応用して鍵系列を生成する様子を示すブロック図である。

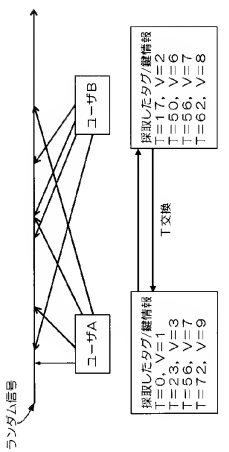
【図１９】本発明の実施例をブロック暗号に応用した構成を示すブロック図である。

【符号の説明】

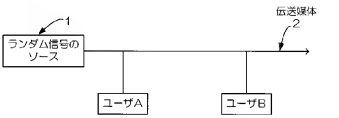
１、１Ａ、１Ｂ・・・ランダム信号のソース
２・・・伝達媒体
２ａ・・・ランダム信号線
２ｂ・・・タグ情報通信線
３・・・サンプリング手段
４・・・ランダム信号採取部
５、５Ｂ、５Ｃ、５Ｄ、５Ｅ・・・分割部
６、６Ｂ・・・タグ／鍵情報格納メモリ

７、７Ｂ・・・制御部
８、８Ｂ、８Ｃ、８Ｅ・・・ランダム信号受信部
９・・・スプリッタ
１０・・・フィルタ
１１、１１Ｃ、１１Ｄ、１１Ｅ・・・Ａ／Ｄ変換手段
１２・・・ランダム信号格納メモリ
１３・・・ランダム信号採取部
１４、１４Ｅ・・・タイミング信号生成部

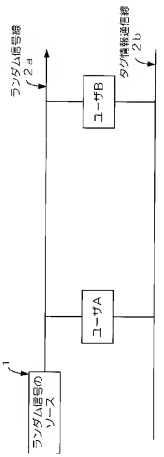
【図１】



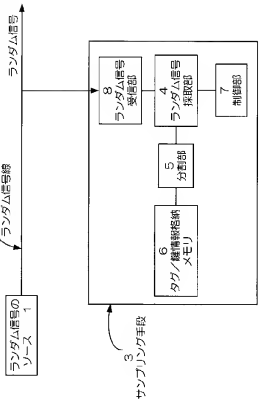
【図２】



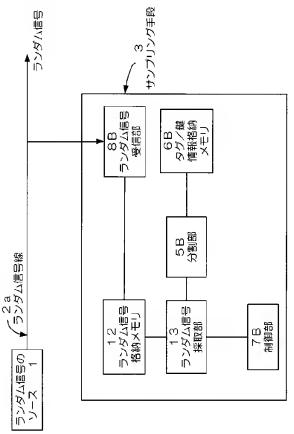
【図３】


ランダム信号線
2a
タグ情報送信線
2b
ユーザB
ユーザA
1
ランダム信号のソース

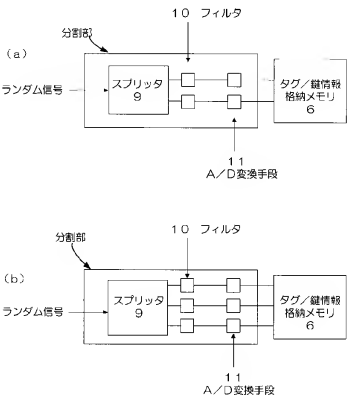
【図４】


ランダム信号
2a
ランダム信号線
ランダム信号のソース
1
8
ランダム信号受信部
4
ランダム信号採取部
7
制御部
5
分割部
6
タグ／鍵情報格納メモリ
3
サンプリング手段

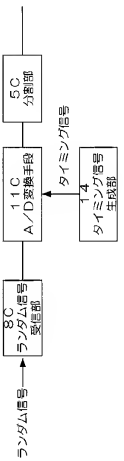
【図５】


ランダム信号
3
サンプリング手段
2a
ランダム信号線
ランダム信号のソース
1
8B
ランダム信号受信部
6B
タグ／鍵情報格納メモリ
5B
分割部
12
ランダム信号格納メモリ
13
ランダム信号採取部
7B
制御部

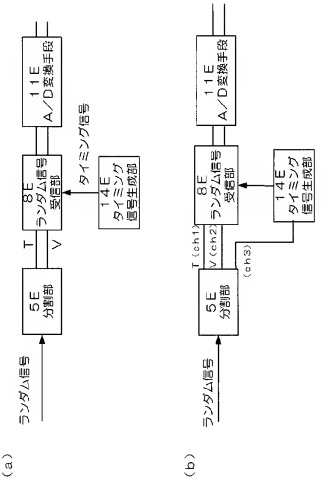
【図６】


(a)
分割部
10 フィルタ
ランダム信号
スプリッタ
9
タグ／鍵情報格納メモリ
6
11
A／D変換手段
(b)
分割部
10 フィルタ
ランダム信号
スプリッタ
9
タグ／鍵情報格納メモリ
6
11
A／D変換手段

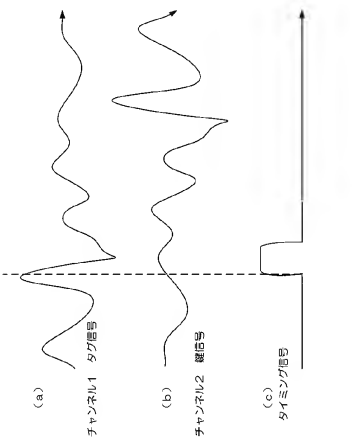
【図７】


ランダム信号
8C
ランダム信号
受信部
11C
A／D変換手段
5C
分割部
タイミング信号
14
タイミング信号
生成部

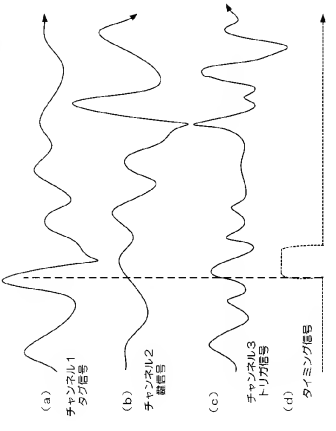
【図８】


(a)
ランダム信号
5E
分割部
T
V
8E
ランダム信号
受信部
11E
A／D変換手段
タイミング信号
14E
タイミング
信号生成部
(b)
ランダム信号
5E
分割部
T (ch1)
V (ch2)
(ch3)
8E
ランダム信号
受信部
11E
A／D変換手段
14E
タイミング
信号生成部

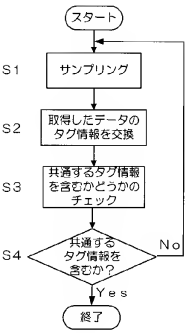
【図９】


(a)
チャンネル1 タグ信号
(b)
チャンネル2 確信号
(c)
タイミング信号

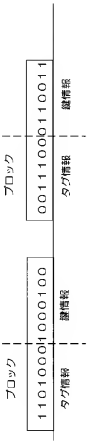
【図１０】


(a)
チャンネル1
タグ信号
(b)
チャンネル2
確信号
(c)
チャンネル3
トリガ信号
(d)
タイミング信号

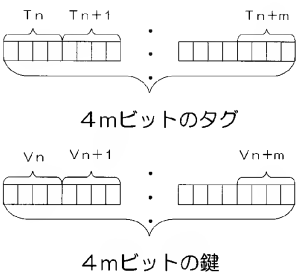
【図１１】



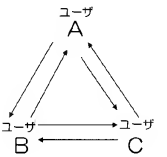
【図１２】



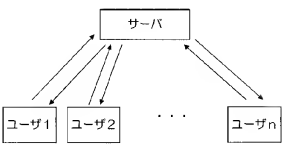
【図１３】



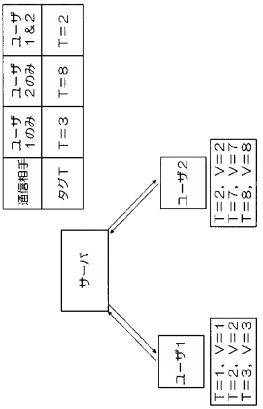
【図１４】



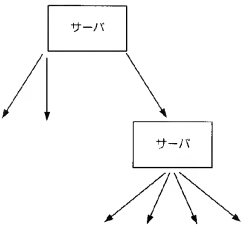
【図１５】



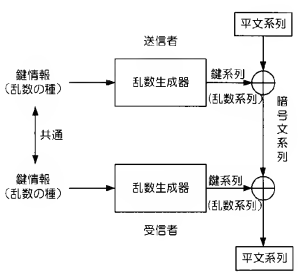
【図１６】



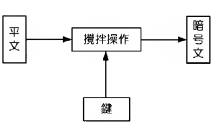
【図１７】



【図１８】



【図１９】



フロントページの続き

(72)発明者 鈴木 亞香
京都府京都市西京区大枝北沓掛町二丁目３番地の１６
(72)発明者 水川 繁光
兵庫県宝塚市小浜５丁目１－１

Ｆターム(参考) 5J104 AA16 EA04 EA08 EA15 NA02